

JENNIFER L. KELLER (SBN 84412)
jkeller@kelleranderle.com
CHASE A. SCOLNICK (SBN 227631)
cscolnick@kelleranderle.com
KELLER ANDERLE SCOLNICK LLP
18300 Von Karman Avenue, Suite 930
Irvine, California 92612
Telephone: (949) 476-8700
Facsimile: (949) 476-0900

Attorneys Plaintiff
GUARDANT HEALTH, INC.

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA
SAN FRANCISCO DIVISION

GUARDANT HEALTH, INC., a Delaware
corporation,

Plaintiff,

v.

NATERA, INC., a Delaware corporation;
ALAN SELEWA, an individual; CATALIN
BARBACIORU, an individual; and DOES 1
through 50, inclusive,

Defendants.

Case No. 3:25-cv-01837

**PLAINTIFF GUARDANT HEALTH, INC.'S
EX PARTE APPLICATION FOR
TEMPORARY RESTRAINING ORDER,
ORDER TO SHOW CAUSE WHY
PRELIMINARY INJUNCTION SHOULD
NOT ISSUE, AND ORDER PERMITTING
EXPEDITED DISCOVERY;
MEMORANDUM OF POINTS AND
AUTHORITIES IN SUPPORT THEREOF**

1 **TO ALL PARTIES AND THEIR ATTORNEYS OF RECORD:**

2 PLEASE TAKE NOTICE that as soon thereafter as the matter may be heard in a courtroom
3 to be determined of the above-entitled Court, located at 280 South 1st Street, San Jose, CA 95113,
4 Plaintiff Guardant Health, Inc. (“Guardant” or “Plaintiff”) will, and hereby does, under Rule 65 of
5 the Federal Rules of Civil Procedure and Local Rule 65-1, apply *ex parte* for: (1) a temporary
6 restraining order against Defendants Alan Selewa and Catalin Barbacioru (collectively, “Employee
7 Defendants”) and Defendant Natera, Inc.; (2) an order to show cause why a preliminary injunction
8 should not issue; and (3) for an order permitting expedited discovery. Because this *ex parte*
9 Application is being filed concurrently with the Complaint, this case has not yet been assigned to a
10 department. Guardant will promptly provide notice to the parties as it is able once it learns of any
11 such assignment.

12 Guardant brings this *ex parte* Application to prevent its ex-employees from exploiting its most
13 valuable research and development trade secrets at a key competitor, Natera. Just before ending their
14 respective employment with Guardant, Employee Defendants accessed and downloaded trade secret
15 and confidential information associated with Guardant’s cutting-edge cancer detection tests.
16 Guardant expended hundreds of millions of dollars and thousands of hours developing the stolen
17 proprietary information and property. This closely held information is not available to competitors
18 or others outside of Guardant and is protected internally through robust non-disclosure agreements
19 and numerous technological security measures.

20 Unless interim injunctive relief is granted through an *ex parte* Application, Guardant will
21 suffer immediate and irreparable harm as Guardant’s most valuable trade secrets will end up in the
22 hands of one of its principal competitors and significantly disadvantage Guardant’s ability to compete.
23 Guardant therefore respectfully requests the Court grant this *ex parte* Application for a temporary
24 restraining order enjoining Defendants and any other person or entity participating with them or acting
25 for, on behalf of, or in concert with them from:

- 26 1. Utilizing, disclosing or using any trade secrets or confidential information belonging to
27 Guardant, including, without limitation, the 6,600 files transferred by Barbacioru to a USB
28 SanDisk 3.2 drive and the 90 files transferred by Selewa to a Google Drive named

1 “Alan_GDrive_Home,” as well as any copies, duplications, or any other materials derivative
2 or created from such files;

3 2. Transferring to any third party any trade secrets or confidential information belonging to
4 Guardant including, without limitation, the items described in 1., above;

5 3. Destroying, altering, deleting, or relinquishing control over to any third party, any and all
6 copies and versions (whether hard copy, native, or electronic) of any documents or
7 electronically stored information on any computer, hard drive, or mobile device (including
8 but not limited to emails, text messages, communications over social media and any other
9 electronic, typewritten, handwritten, recorded, or printed matter of any kind) relating to the
10 items described in 1., above;

11 4. Violating or aiding or participating in the violation of any of the terms of Employee
12 Defendants their respective Confidential Information and Invention Assignment Agreements
13 (“CIAAs”), as described in the Complaint and attached to the Declaration of Steven Mancini
14 filed with the *ex parte* Application.

15 Guardant also respectfully requests an order to show cause why a preliminary injunction
16 should not issue enjoining and imposing the same restrictions as set forth above.

17 Guardant also respectfully requests an order requiring Employee Defendants, and each of
18 them, within three (3) business days, to return to Guardant, through Guardant’s counsel of record:

19 1. Guardant’s trade secret and confidential information, including all files downloaded,
20 copied, or removed by Employee Defendants, including those on the USB SanDisk 3.2 drive and
21 Google Drive named “Alan_GDrive_Home” described above;

22 2. Any devices, drives, computers, tablets, phones, electronic media, emails and email
23 accounts, and cloud storage that contain Guardant’s trade secret and confidential information; and

24 3. A declaration signed under oath (i) verifying that the Employee Defendant has
25 returned all of Guardant’s trade secret and confidential information to Guardant, (ii) verifying that
26 the Employee Defendant has not retained any copies, duplications, or any other materials derivative
27 or created from Guardant’s trade secret and confidential information, and (iii) identifying all person(s)
28

1 to whom the Employee Defendant shared with, provided access to, transferred to, or otherwise
2 disclosed Guardant's trade secret and confidential information before such return to Guardant.

3 Finally, Guardant requests that the Court issue an order for expedited discovery so Guardant
4 may conduct narrowly tailored discovery to determine:

5 1. The company property Employee Defendants took from Guardant, including the trade
6 secret and confidential information that is the subject of this action;

7 2. The current location of all Guardant property taken by the Employee Defendants,
8 including the trade secret and confidential information that is the subject of this action;

9 3. Whether, when and what trade secret and confidential information Employee
10 Defendants have disclosed to their new employer, Natera;

11 4. Whether and what trade secret and confidential information Employee Defendants are
12 using in their employment at Natera;

13 5. Whether Employee Defendants engaged in any communications with any other former
14 Guardant employees that related to Guardant's proprietary information; and

15 6. Allowing a forensic computer examination of all computers to which Employee
16 Defendants had access or which the Employees used to access, review, or copy Guardant's proprietary
17 information.

18 This *ex parte* Application is based on the Complaint, the Memorandum of Points and
19 Authorities, the Declarations of Chase Scolnick, Dr. Stefanie Mortimer, and Steven Mancini, and the
20 exhibits thereto; the Proposed Order, and such other evidence and argument that the court may
21 consider at the hearing of the Application.

22 Notice of this *ex parte* Application has been given under Local Rule 65-1 by sending
23 Defendants a copy of the Complaint, this *ex parte* Application, the following Memorandum of Points
24 and Authorities, the Declarations and the exhibits thereto, and the Proposed Order by email to
25 Employee Defendants' last known email address, and also by Federal Express delivery by a registered
26 process service to their last known place of employment (Natera), and to Defendant Natera by service
27 on its agent for service of process any by email to its general counsel's office. *See* Decl. of Chase
28 Scolnick in Support of Guardant's Application for a Temporary Restraining Order, Order to Show

1 Cause Why Preliminary Injunction Should Not Issue, and Order Permitting Expedited Discovery, ¶
2 3.

3 Respectfully submitted,

4 Dated: February 20, 2025

KELLER ANDERLE SCOLNICK LLP

5 By: /s/ Chase A. Scolnick
6 Chase A. Scolnick

7 Attorneys for Plaintiff
8 GUARDANT HEALTH, INC.
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

TABLE OF CONTENTS

I.	INTRODUCTION	1
II.	FACTUAL BACKGROUND.....	2
A.	Guardant Is The Leading Provider Of Cancer Detection Blood Tests	2
B.	Guardant’s Trade Secrets Are The Lifeblood Of Its Business	3
C.	Natera Is Guardant’s Competitor But Has Not Been Able To Successfully Develop Its Own Tests. Natera Therefore Has Targeted Guardant’s Employees And Trade Secrets.....	5
D.	Natera Employs A Scheme By Which Selewa And Barbacioru Take Guardant’s Trade Secrets For Natera’s Benefit.....	5
III.	LEGAL STANDARD.....	7
IV.	ARGUMENT	7
A.	Guardant Is Likely To Succeed On The Claims In Its Complaint.....	8
1.	DTSA & CUTSA	8
a.	The Information Employee Defendants Took Constitute Guardant’s Trade Secrets.....	8
b.	Defendants Misappropriated Guardant’s Property	11
c.	Guardant Has Been Harmed	12
d.	Guardant Overwhelming Satisfies This Factor—Likelihood of Success—For Issuing A TRO On Its DTSA and CUTSA.....	12
2.	Breach of Contract Claim	13
B.	Irreparable Harm.....	14
C.	Balance of Equities	15
D.	Injunction is the Public Interest	15
E.	Bond.....	15
F.	Guardant needs expedited discovery to determine the scope of Defendants’ use and dissemination of Guardant’s Trade Secrets and Confidential Information.....	16
V.	CONCLUSION.....	17

TABLE OF AUTHORITIES

Cases

<i>Agency Solutions.Com, LLC v. TriZetto Group, Inc.</i> , 819 F. Supp. 2d 1001 (E.D. Cal. 2011).....	11
<i>Albert’s Organics, Inc. v. Holzman</i> , 2020 WL 1332074 (N.D. Cal. Mar. 23, 2020).....	14
<i>Alliance for the Wild Rockies v. Cottrell</i> , 632 F.3d 1127 (9th Cir. 2011)	7
<i>Alta Devices, Inc. v. LG Elecs., Inc.</i> , 343 F. Supp. 3d 868 (N.D. Cal. 2018)	8
<i>Apple Inc. v. Rivos, Inc.</i> , 2023 WL 5183034 (N.D. Cal. Aug. 11, 2023)	14
<i>Bank of Am., N.A. v. Lee</i> , 2008 WL 4351348 (C.D. Cal. Sept. 22, 2008)	15
<i>Comet Techs. USA v. Beuerman</i> , 2018 WL 1990226 (N.D. Cal. 2018)	passim
<i>CytoDyn of New Mexico, Inc. v. Amerimmune Pharm., Inc.</i> , 160 Cal. App. 4th 288 (2008)	8
<i>Doe v. San Diego Unified Sch. Dist.</i> , 19 F.4th 1173 (9th Cir. 2021).....	7
<i>Eldorado Stone, LLC v. Renaissance Stone, Inc.</i> , 2005 WL 5517732 (S.D. Cal. May 31, 2005)	10, 14
<i>Eurofins Elec. and Electronic Testing NA, LLC v. SGS N. Am.</i> , 2024 WL 4197635 (N.D. Cal. Sep. 12, 2024).....	10
<i>First Comm’l Mortg. Co. v. Reece</i> , 89 Cal. App. 4th 731 (2001)	13
<i>Fitspot Ventures, LLC v. Bier</i> , 2015 WL 5145513 (C.D. Cal. Sept. 1, 2015)	11, 16
<i>Grooms v. Legge</i> , 2009 WL 704644 (S.D. Cal. Mar. 17, 2009).....	17
<i>Henry Schein, Inc. v. Cook</i> , 191 F. Supp. 3d 1072 (N.D. Cal. 2016)	passim
<i>Insider Software, Inc. v. ID Designs, Inc.</i> , 2020 WL 5094842 (N.D. Cal. Aug. 28, 2020).....	8
<i>Jorgensen v. Cassidy</i> , 320 F. 3d 906 (9th Cir. 2003).....	15
<i>KLA–Tencor Corp. v. Murphy</i> , 717 F. Supp. 2d 895 (N.D. Cal. 2010).....	7, 17
<i>Kwikset Corp. v. Super. Ct.</i> , 51 Cal. 4th 310 (2010)	11
<i>Lillge v. Verity</i> , 2007 WL 2900568 (N.D. Cal. Oct. 2, 2007).....	14
<i>Morlife, Inc. v. Perry</i> , 56 Cal. App. 4th 1514 (1997)	15
<i>Oakwood Laboratories LLC v. Thanoo</i> , 999 F.3d 892 (9th Cir. 2021)	12
<i>Posdata Co. v. Kim</i> , 2007 WL 1848661 (N.D. Cal. 2007)	8, 10, 14
<i>Pyro Spectaculars N., Inc. v. Souza</i> , 861 F. Supp. 2d 1079 (E.D. Cal. 2012)	15, 17
<i>Semitool, Inc. v. Tokyo Electron Am., Inc.</i> , 208 F.R.D. 273 (N.D. Cal. 2002).....	16

1	<i>Silvaco Data Sys. v. Intel Corp.</i> , 184 Cal. App. 4th 210 (2010).....	11
2	<i>Space Data Corp. v. X</i> , 2017 WL 5013363 (N.D. Cal. Feb. 16, 2017)	8
3	<i>Stuhlbarg Int’l Sales Co. v. John D. Brush & Co.</i> , 240 F.3d 832, n. 7 (9th Cir. 2001).....	7, 14
4	<i>TMX Funding, Inc. v. Impero Techs., Inc.</i> , 2010 WL 1028254 (N.D. Cal. 2010).....	10
5	<i>TMX Funding, Inc. v. Impero Techs., Inc.</i> , 2010 WL 1028254 (N.D. Cal. Mar. 18, 2010)	14
6	<i>W. Directories, Inc. v. Golden Guide Directories, Inc.</i> , 2009 WL 1625945 (N.D. Cal. 2009)	14
7	<i>Winter v. Natural Res. Def. Council, Inc.</i> , 555 U.S. 7 (2008)	7
8	Statutes	
9	18 U.S.C. § 1839(3)	8
10	18 U.S.C. § 1839(5)	8, 11
11	18 U.S.C. § 1839(6)	11
12	Cal. Civ. Code § 3426.1(a)	11
13	Cal. Civ. Code § 3426.1(b)	8, 11
14	Cal. Civ. Code § 3426.1(d)	9

1 **I. INTRODUCTION**

2 By this *ex parte* application, Guardant seeks urgent, extraordinary relief. But the relief
3 Guardant seeks is overwhelmingly justified and warranted by the misconduct of Defendant Natera,
4 Inc. and two former Guardant employees who Natera has entangled in its efforts to obtain Guardant's
5 trade secrets. In recent days, Defendants Alan Selewa and Catalin Barbacioru (collectively,
6 "Employee Defendants") left their employment at Guardant to go to Natera, but only after collectively
7 transferring over 6,600 confidential, trade secret files from Guardant's IT network to their own
8 personal storage locations on their way out the door.

9 Guardant has developed groundbreaking early cancer blood tests, and continues to work on
10 developing even greater technologies. The files taken by Employee Defendants concern highly
11 confidential, non-public information covering many critical aspects of Guardant's development
12 efforts on both recent and ongoing projects—*e.g.*, original source code, research parameters, genome
13 biomarker identifiers, testing specifications, and algorithm details. That such information has
14 significant economic value to Guardant—and would have such value to competitors like Natera if it
15 fell into their hands—cannot reasonably be disputed. The Employee Defendants signed
16 confidentiality agreements at the outset of their employment with Guardant, leaving no doubt as to
17 the sensitivity of such information and the strict prohibition on it being removed from Guardant's
18 premises or network.

19 The need for emergency injunctive relief is clear. Promptly upon learning of Employee
20 Defendants' theft, and the scheme to transfer Guardant's trade secrets, Guardant filed this action and
21 this application. As set forth in the supporting declarations of Steve Mancini and Dr. Stefanie
22 Mortimer, Employee Defendants took a large volume of confidential material that not only constituted
23 misappropriation of trade secrets under both federal and state law but breached explicit confidentiality
24 agreements. There is no possible justification for this improper transfer, nor does Natera have any
25 right to any of this information.

26 Guardant is likely to succeed on the merits of its claims. Absent immediate injunctive relief,
27 Employee Defendants and Natera may further misappropriate, disclose, or use Guardant's highly
28 confidential trade secrets for their own gain, which would only aggravate Defendants' wrongdoing

1 and irreparably harm Guardant. In contrast, Employee Defendants and Natera have no possible
2 legitimate claim to possess or use Guardant’s trade secrets and hardly could be harmed by an order
3 requiring them to mitigate their wrongdoing and abide by the law.

4 Guardant therefore requests that the Court grant this application, issue a temporary restraining
5 order prohibiting all Defendants from disclosing or using Guardant’s confidential information and
6 trade secrets in any way and to immediately return them without retaining any copies, and authorize
7 narrow, expedited discovery to allow Guardant to determine the scope of Employee Defendants’
8 misappropriation and whether there has been any additional dissemination of Guardant’s sensitive
9 information.

10 **II. FACTUAL BACKGROUND**

11 **A. Guardant Is The Leading Provider Of Cancer Detection Blood Tests**

12 Since being founded in 2012, Guardant has focused its expertise on developing liquid biopsy
13 assays for cancer. Compl., ¶ 9; Mortimer Decl., ¶¶ 2-3. Cancer results from abnormal cells that
14 develop into a tumor, which increasingly sheds cell fragments into the bloodstream known as
15 circulating tumor DNA (“ctDNA”) as it grows. Compl., ¶ 20. Guardant was the first company to
16 develop and commercialize a liquid biopsy assay to identify genomic biomarkers for advanced solid
17 tumors using cell-free ctDNA, from simple, non-invasive blood draws. *Id.*, ¶ 9; Mortimer Decl., ¶ 3.

18 One of Guardant’s focuses has been the development of blood draw assays that can detect
19 cancer as early as possible, which requires identifying and classifying even smaller fragments of
20 ctDNA in the blood. *Id.*, ¶ 20. Guardant has blazed the trail for early cancer detection and developed
21 a product called “Shield,” which is the first blood test approved by the FDA as a primary screening
22 option for colorectal cancer. *Id.*, ¶ 21.

23 Since releasing Shield, Guardant has worked to develop an even more comprehensive early
24 cancer blood test—a multi-cancer classifier and cancer of origin identifier for screening use. *See*
25 Mortimer Decl., ¶ 6. In its development stage, Guardant refers to this project as “MCD” (multi-cancer
26 detection”) or “MCED” (multi-cancer early detection) test. *Id.*; Compl., ¶ 23. This test would be able
27 to detect and identify unique markers in the ctDNA found in a blood sample that would allow
28 clinicians to identify the type of cancer and the location of the tumor in the patient. Mortimer Decl.,

¶¶ 7-8, 10-11; Compl., ¶ 23. This would be a revolutionary screening tool in the medical field, as it would allow patients to determine from a routine blood draw whether they have any early indication of numerous forms of cancer and, if so, the origin of the cancer. *Id.*

B. Guardant's Trade Secrets Are The Lifblood Of Its Business

Guardant's cancer detection products take years and millions of dollars to develop and bring to market. Like the development of any medical test, the research and development phase for Guardant's products includes substantial trial and error, dead ends, breakthroughs, and validations. *See* Mortimer Decl., ¶ 10. Guardant's products are built off a knowledge and experience base guided as much by what does not work, as what does. *Id.*, ¶¶ 3, 6-11. Throughout the development process of its products (including Shield and MCED), Guardant creates, owns, and maintains confidential, proprietary, trade secret information, data, and technology not known to the public and which has substantial economic value from not being known to others ("Trade Secrets"). *Id.*; Mancini Decl., ¶¶ 2-9. These Trade Secrets include:

- Proprietary computer software, systems, and data used to determine, update, and maintain validations for sample testing, including proprietary knowledge and calculations for determining sample types, dilution approaches, acceptance criteria, and other factors used to calibrate testing conditions and factors affecting accuracy of testing;
- Proprietary research, data, summaries, results, algorithms, and similar internal specifications for probes and probe testing, which are used for virtually all of Guardant's products to (1) help identify the region or regions of the genomes being examined in developing accurate testing, which occurs through time-consuming and expensive work including trial and error, (2) create "blacklists" denoting problematic regions of the genome that require further investigation and research, and (3) identify filters for Guardant's algorithms to address those "blacklists" and help identify biomarkers within the genomes;
- Internal source code used in Guardant's algorithms developed to permit a blood test to operate successfully, *e.g.*, algorithm instructions triggering the test to identify biomarkers indicative of early cancer in the blood genome being tested; and

- Internal descriptions, data, presentations, summaries, and compilations describing how Guardant’s testing applications and callers (*i.e.*, triggers for identifying the condition being tested) work and operate and, importantly, those that were tested and developed but did not work or operate sufficiently.

See Compl., ¶ 24; Mortimer Decl., ¶¶ 3-11; Mancini Decl., ¶¶ 3-9. Taken together, these Trade Secrets lay out the design, research and development, test methods and results, quality and accuracy assurances, and source code processes of its cancer-detecting blood tests. *Id.* If disclosed to a competitor or other third party, they would understand how Guardant’s tests work, what progress it has made on developing successful tests, what works and what does not work, and how to implement and commercialize that knowledge base into useful testing apparatuses. *Id.*

Guardant takes extreme precautions to ensure the confidentiality of its Trade Secrets. Guardant’s IT systems are secured to limit access to its Trade Secrets and protect against any untoward or suspicious activity regarding those Trade Secrets. *See* Mancini Decl., ¶¶ 4-8. These protections include (a) physical, online, and other electronic security features to ensure confidential and proprietary documents and information cannot be accessed by any unauthorized person or entity; (b) dissemination of Trade Secret information only on an “as needed” basis; and (c) ensuring all employees or agents with access to the Trade Secrets agree to maintain their confidentiality, most often in a written confidentiality agreement. *See id.*; Compl., ¶ 25.

Like other employees in their position, Selewa and Barbacioru signed “Confidential Information and Invention Assignment Agreement (“CIIAAs”) with Guardant. *See* Mancini Decl., ¶¶ 6-7, Exs. A, B. Through these CIIAAs, Selewa, Barbacioru and other employees agree “at all times in perpetuity to hold all Confidential Information in confidence and to not disclose, use, copy, publish, summarize, or remove from the premises of the Company any Confidential Information,” with “Confidential Information” broadly defined to include “all information and materials that are confidential, secret, or proprietary (whether or not technical in nature) related to any aspect of the business of the Company.”¹ *Id.* The CIIAAs also require the employee to return to Guardant and not

¹ The CIIAAs include carve outs where the employee needs to disclose or use Confidential Information “as necessary to carry out my assigned responsibilities as a Company employee” or “after termination . . . only as specifically authorized in writing by an officer of the Company.” *See* Mancini

1 keep any devices, records, data, or other company documents or property, whether confidential or
2 not, upon termination and to sign a “Termination Certification” to that effect. *Id.*

3 The use of and provisions in the CIIAAs ensure employees understand the sensitivity of
4 Guardant’s confidential information, including the Trade Secrets, and agree to preserve, protect, and
5 not use them. *Id.*

6 **C. Natera Is Guardant’s Competitor But Has Not Been Able To Successfully**
7 **Develop Its Own Tests. Natera Therefore Has Targeted Guardant’s Employees**
8 **And Trade Secrets**

9 Natera is a competitor of Guardant but has been unable to develop or launch any early cancer
10 blood tests. In response to Guardant’s success in this space, Natera has targeted and recruited
11 Guardant’s employees aggressively in an effort to jumpstart its lagging position. Natera’s approach
12 has led it to not only poach Guardant’s employees but also Guardant’s Trade Secrets.

13 Among those Guardant employees Natera recently targeted and hired are Alan Selewa and
14 Catalin Barbacioru. *See* Compl., ¶¶ 30-32; Mortimer Decl., ¶ 5; Mancini Decl., ¶ 9. Selewa left
15 Guardant for Natera in late January 2025, and Barbacioru left Guardant for Natera in early February
16 2025. *Id.* While at Guardant, both Selewa and Barbacioru worked on Guardant’s oncology products,
17 including its early cancer detection blood tests. *Id.*

18 Following their departures, Guardian performed a computer investigation and audit that
19 revealed each took Guardant’s Trade Secrets with them, as detailed below. *See* Mancini Decl., ¶ 9.
20 Selewa’s and Barbacioru’s defections in the last few days and weeks follow Natera’s recruitment and
21 hiring in recent months of three other bioinformatic scientists who had worked at Guardant, including
22 Princy Parsana (“Parsana”), Sofia Medina Ruiz (“Ruiz”), and Swati Goyal (“Goyal”). *See* Compl., ¶
23 34.

24 **D. Natera Employs A Scheme By Which Selewa And Barbacioru Take Guardant’s**
25 **Trade Secrets For Natera’s Benefit**

26 Guardant conducted a computer and forensic investigation after Selewa’s and Barbacioru’s
27 departures. *See* Mancini Decl., ¶ 9. What Guardian discovered was deeply concerning. In the days
28 before his departure, Selewa transferred approximately 90 files containing Guardant’s Trade Secrets

Decl., ¶¶ 6-7, Exs. A, B. Here, neither Selewa nor Barbacioru had authorization to disclose, keep, use, or remove any Confidential Information after their terminations from Guardant.

1 and Confidential Information from Guardant’s IT systems to Selewa’s personal Google storage drive
2 (“Selewa GDrive”). *See id.*; Mortimer Decl., ¶¶ 5-11. And, just days before his departure, Barbacioru
3 moved approximately 6,500 files containing Guardant’s Trade Secrets and Confidential Information
4 from Guardant’s network to an external USB hard drive (“Barbacioru USB Drive”). *Id.*

5 The files and data transfers to the Selewa GDrive and Barbacioru USB Drive include all types
6 of Guardant’s Trade Secrets described above. *See* Mortimer Decl., ¶¶ 6-11. The transferred files
7 include models for Guardant’s MCD/MCED tests, including internal analyses and evaluations of the
8 results and interpretations of the tests. *Id.*, ¶ 6. They include original source code Guardant’s newly
9 initiated tissue informed or tissue enhancing modeling efforts. *Id.*, ¶ 7. They include files related to
10 ways Guardant has worked to improve the accuracy of its tests by analyzing the test results in
11 comparison to other biomarkers. *Id.*, ¶ 8. They include technical details for how Guardant performs
12 validations for its products. *Id.*, ¶ 9. They include files for probes for nearly all of Guardant’s
13 products, including the specific regions of the human genome Guardant is targeting with its tests and
14 analyses. *Id.*, ¶ 10. They include “blacklists” that reflect how Guardant filters problematic regions
15 in its different algorithms. *Id.* They include files reflecting different callers for Guardant’s tests that
16 act as triggers for identification of conditions being tested. *Id.*, ¶ 11. The files taken by Barbacioru
17 include files related to projects on which Barbacioru did not work. Compl., ¶ 43.

18 Guardant does not have access to the Selewa GDrive or Barbacioru USB Drive and cannot
19 know the full extent or scope to which that information has been disclosed, disseminated, or used.
20 But the only logical conclusion is that Selewa and Barbacioru took this information for use in their
21 new employment at Natera. Selewa and Barbacioru had no reason or purpose to take Guardant’s
22 Trade Secrets other than to use at Natera, who would be the ultimate beneficiary. And, based on the
23 timing and Selewa and Barbacioru’s intentional misappropriation, it appears highly likely Natera
24 hired Selewa and Barbacioru specifically due to their work on and access to Guardant’s early cancer
25 blood test products and other Trade Secrets and with direction, knowledge, and guidance for them to
26 take Guardant’s Trade Secrets on their way out.

27 Notably, this is not the first time Natera has stepped over the line in their efforts to unfairly
28 compete with Guardant. In November 2024, a jury in this District awarded Guardant \$292.5 million,

1 including \$175.5 million in punitive damages, on Guardant’s Lanham Act false advertising claims
2 against Natera. *See* Scolnick Decl., ¶ 4. The jury found Natera engaged in a deliberate campaign to
3 mislead cancer clinicians about Guardant’s “Reveal” test, which detects early colorectal cancer, in
4 favor of Natera’s product. *Id.* The jury also rejects all of Natera’s counterclaims. *Id.*

5 **III. LEGAL STANDARD**

6 The standard for issuing a TRO is the same as that for issuing a preliminary injunction,
7 *Stuhlbarg Int’l Sales Co. v. John D. Brush & Co.*, 240 F.3d 832, n. 7 (9th Cir. 2001), which requires
8 the plaintiff to establish: (1) likelihood of success on the merits; (2) likelihood of irreparable harm in
9 the absence of preliminary relief; (3) that the balance of equities tips in his favor; and (4) that an
10 injunction is in the public interest. *See Winter v. Natural Res. Def. Council, Inc.*, 555 U.S. 7, 20
11 (2008). The Ninth Circuit has held that “‘serious questions going to the merits’ and a hardship balance
12 that tips sharply toward the plaintiff can support issuance of an injunction, assuming the other two
13 elements of the Winter test are also met.” *See Alliance for the Wild Rockies v. Cottrell*, 632 F.3d
14 1127, 1132 (9th Cir. 2011).

15 Courts in the Ninth Circuit “appl[y] a ‘sliding scale’ approach to preliminary injunctions such
16 that a preliminary injunction can issue ‘where the likelihood of success is such that “serious questions
17 going to the merits were raised and the balance of hardships tips sharply in plaintiff’s favor.” *Doe v.*
18 *San Diego Unified Sch. Dist.*, 19 F.4th 1173, 1177 (9th Cir. 2021) (cleaned up).

19 **IV. ARGUMENT**

20 Courts in this district routinely grant TROs in cases like this involving employees leaving
21 their former employer and taking trade secrets with them to their new employer. *See, e.g., Henry*
22 *Schein, Inc. v. Cook*, 191 F. Supp. 3d 1072, 1077 (N.D. Cal. 2016) (granting TRO where former
23 employee had “e-mailed and downloaded, to her personal devices, confidential information from [her
24 former employer] before leaving her employment to work at a competitor”); *KLA–Tencor Corp. v.*
25 *Murphy*, 717 F. Supp. 2d 895, 898 (N.D. Cal. 2010) (in case alleging trade secret misappropriation
26 by former employees, court ordered temporary restraining order prohibiting defendants from
27 destroying evidence and requiring defendants to preserve electronic evidence); *Comet Techs. USA v.*
28 *Beuerman*, 2018 WL 1990226, *3 (N.D. Cal. 2018) (granting TRO against former employee);

1 *Posdata Co. v. Kim*, 2007 WL 1848661, at *5 (N.D. Cal. 2007) (granting TRO against former
2 employee and new employer). Given the conclusive evidence both Employee Defendants
3 misappropriated trade secrets upon their departure from Guardant and are now working at one of
4 Guardant’s primary competitors, Guardant requests the Court do the same here and enter the requested
5 TRO.

6 **A. Guardant Is Likely To Succeed On The Claims In Its Complaint.**

7 1. DTSA & CUTSA

8 To demonstrate trade secret misappropriation under the DTSA and the CUTSA, a plaintiff
9 must show that: “(1) the plaintiff owned a trade secret; (2) the defendant misappropriated the trade
10 secret; and (3) the defendant's actions damaged the plaintiff.” *Alta Devices, Inc. v. LG Elecs., Inc.*,
11 343 F. Supp. 3d 868, 877 (N.D. Cal. 2018) (quoting *Space Data Corp. v. X*, 2017 WL 5013363, at *2
12 (N.D. Cal. Feb. 16, 2017)); *CytoDyn of New Mexico, Inc. v. Amerimmune Pharm., Inc.*, 160 Cal. App.
13 4th 288, 297 (2008); see also 18 U.S.C. § 1839(5); Cal. Civ. Code § 3426.1(b). “The elements of
14 misappropriation under the DTSA are similar to those under the CUTSA.” *Alta Devices*, 343 F. Supp.
15 3d at 877 (quoting *Space Data Corp.*, 2017 WL 5013363, at *2). “Actual or threatened
16 misappropriation may be enjoined.” *Insider Software, Inc. v. ID Designs, Inc.*, 2020 WL 5094842,
17 at *3 (N.D. Cal. Aug. 28, 2020) (citation omitted).

18 **a. The Information Employee Defendants Took Constitute Guardant’s**
19 **Trade Secrets**

20 The DTSA defines a “trade secret” as “financial, business, scientific, technical, economic, or
21 engineering information” that “(A) the owner thereof has taken reasonable measures to keep ... secret;
22 and (B) ... derives independent economic value, actual or potential, from not being generally known
23 to, and not being readily ascertainable through proper means by, another person who can obtain
24 economic value from the disclosure or use of the information.” 18 U.S.C. § 1839(3). Similarly,
25 CUTSA defines a “trade secret” as “information, including a formula, pattern, compilation, program,
26 device, method, technique, or process that: (1) [d]erives independent economic value, actual or
27 potential, from not being generally known to the public or to other persons who can obtain economic
28

1 value from its disclosure or use; and (2) [i]s the subject of efforts that are reasonable under the
2 circumstances to maintain its secrecy.” Cal. Civ. Code § 3426.1(d).

3 Based on the forensic examination of its computer systems Guardant conducted after the
4 Employee Defendants’ departure, Guardant determined the Employee Defendants misappropriated,
5 in summary:

- 6 • Guardant’s internal source code used for its algorithms developed to permit a blood test
7 to operate successfully;
- 8 • Guardant’s internal software and data used to maintain validations for sample testing,
9 including the specific knowledge of and calculations for determining sample types,
10 acceptance criteria, and other factors used to calibrate Guardant’s tests, including which
11 factors affect those tests;
- 12 • Guardant’s research, data, algorithms, and specifications for probes and probe testing,
13 based on extensive trial and error, and which are used for virtually all of Guardant’s
14 products;
- 15 • Internal data, presentations, and compilations describing in detail how Guardant’s tests
16 and the triggers in those tests operate, including potential triggers tested and developed
17 but did not work or operate sufficiently.

18 *See* Compl., ¶ 24; Mortimer Decl., ¶¶ 4-11; Mancini Decl., ¶ 9. Taken together, these Trade Secrets
19 lay out the design, research and development, test methods and results, quality and accuracy
20 assurances, and source code processes of its cancer-detecting blood tests. *Id.* If disclosed to a
21 competitor or other third party, they would understand how Guardant’s tests work, what progress it
22 has made on developing successful tests, what works and what does not work, and how to implement
23 and commercialize that knowledge base into useful testing apparatuses. *Id.*

24 These Trade Secrets therefore derive value from not being generally known outside Guardant.
25 And, as courts have held, “[a] collection of data that allows the holder to recreate one of Plaintiff’s
26 top technologies derives its value from not being generally known, because Plaintiff’s competitive
27 edge would evaporate if the public and its competitors could easily recreate its products.” *Comet*
28 *Techs. USA v. Beuerman*, 2018 WL 1990226, *3 (N.D. Cal. 2018); *Posdata*, 2007 WL 1848661, at

*1, 4–5 (finding for TRO purposes that Plaintiff was likely to show the design for a computer chip constituted a trade secret); *Eldorado Stone, LLC v. Renaissance Stone, Inc.*, 2005 WL 5517732, at *2-3 (S.D. Cal. May 31, 2005) (finding for preliminary injunction purposes that information an employee copied that showed “the exact way that Eldorado makes each of its products” constituted a trade secret).

Moreover, Guardant took significant efforts to protect its confidential and trade secret information far more stringent than the bare “reasonable measures” DTSA and CUTSA require. For example, Guardant’s IT systems are secured to limit access to its Trade Secrets and protect against any untoward or suspicious activity regarding those Trade Secrets. *See Mancini Decl.*, ¶¶ 4-8. These protections include (a) physical, online, and other electronic security features to ensure confidential and proprietary documents and information cannot be accessed by any unauthorized person or entity; (b) dissemination of Trade Secret information only on an “as needed” basis; and (c) ensuring all employees or agents with access to the Trade Secrets agree to maintain their confidentiality, most often in a written confidentiality agreement. *See id.* Guardant’s efforts to protect its data go well beyond just “reasonable measures.” *See Comet Techs.*, 2018 WL 1990226 at *3 (holding that requiring employees to sign NDAs, conducting exit interviews stressing confidentiality obligations, establishing internal policies, and using technological measures to limit access to and dissemination of data constituted “reasonable measures”); *Posdata*, 2007 WL 1848661, at *5 (finding for TRO purposes that confidentiality agreements and internal security procedures were reasonable measures); *TMX Funding, Inc. v. Impero Techs., Inc.*, 2010 WL 1028254, at *4 (N.D. Cal. 2010) (finding for preliminary injunction purposes that confidentiality agreements and password protections constituted reasonable measures).

The materials Employee Defendants misappropriated are precisely the kinds of trade secrets CUTSA and DTSA are designed to protect. *See, e.g., Eurofins Elec. and Electronic Testing NA, LLC v. SGS N. Am.*, 2024 WL 4197635, *1-2 (N.D. Cal. Sep. 12, 2024) (finding a wireless testing lab’s protected information regarding its test chambers layout, equipment specifications, testing results, pricing information, and other client information constituted trade secrets under DTSA and CUTSA because it would derive economic value from remaining confidential from the lab’s competitors);

1 *Comet Techs.*, 2018 WL 1990226, at *1-3 (holding protected documents related to an upcoming
2 project that would, if disclosed, allow another company to erode the owner’s competitive edge were
3 trade secrets under DTSA and CUTSA); *Agency Solutions.Com, LLC v. TriZetto Group, Inc.*, 819 F.
4 Supp. 2d 1001, 1017 (E.D. Cal. 2011) (“source code is undoubtedly a trade secret” under California
5 law); *Fitspot Ventures, LLC v. Bier*, 2015 WL 5145513, at *3 (C.D. Cal. Sept. 1, 2015); *see also*
6 *Silvaco Data Sys. v. Intel Corp.*, 184 Cal. App. 4th 210, 218 (2010), disproved on other grounds by
7 *Kwikset Corp. v. Super. Ct.*, 51 Cal. 4th 310 (2010) (“the source code for many if not most commercial
8 software products is a secret,”).

9 **b. Defendants Misappropriated Guardant’s Property**

10 Despite Guardant’s substantial efforts, before their departure, Employee Defendants accessed
11 Guardant’s systems to obtain Guardant’s Trade Secrets and other proprietary and confidential data
12 they were forbidden from retaining. Under both the DTSA and the CUTSA, this constitutes
13 “misappropriation.” Misappropriation is (1) the “[a]cquisition of a trade secret by another person
14 who knows or has reason to know that the trade secret was acquired by improper means;” or (2) the
15 “[d]isclosure or use of a trade secret of another without express or implied consent.” 18 U.S.C. §
16 1839(5); Cal. Civ. Code § 3426.1(b). Both the DTSA and CUTSA define “improper means” to
17 include “theft, bribery, misrepresentation, breach or inducement of a breach of a duty to maintain
18 secrecy, or espionage through electronic or other means....” 18 U.S.C. § 1839(6); Cal. Civ. Code §
19 3426.1(a).

20 Here, after the Employee Defendants departed, Guardant conducted a computer and forensic
21 investigation using the monitoring software it installs on all of its employees’ computers. *See* Mancini
22 Decl., ¶ 9. Guardant discovered that Selewa had transferred approximately 90 files containing
23 Guardant’s Trade Secrets and Confidential Information to his personal Google storage drive. *Id.*
24 Likewise, Barbacioru moved 6,600 files containing Guardant’s Trade Secrets and Confidential
25 Information from Guardant’s network to an external USB hard drive. *Id.*

26 The investigation further confirmed the files and data transfers included all types of
27 Guardant’s Trade Secrets described above, including, for example: source code for Guardant’s
28 oncology tests and algorithms; validation parameters and specifications for Guardant’s blood tests;

1 “blacklists” showing biomarkers in identified genomes; internal summaries, compilations, and
2 presentation about the status of Guardant’s product development efforts; and how Guardant’s
3 applications and testing callers operate. *See* Mortimer Decl., ¶¶ 6-11. The files Barbacioru took
4 include such information about virtually all of Guardant’s diagnostic tests, even though Barbacioru
5 did not work on many of those projects and does not appear to have had any legitimate purpose or
6 need to access those files even while working at Guardant.

7 **c. Guardant Has Been Harmed**

8 Defendants’ misappropriation undeniably has harmed Guardant. That Employee Defendants
9 and Natera have not yet launched a competing product does not show the absence of harm. *See, e.g.,*
10 *Oakwood Laboratories LLC v. Thanoo*, 999 F.3d 892, 913-914 (9th Cir. 2021). As the Ninth Circuit
11 has found, “[b]y statutory definition, trade secret misappropriation *is* harm.” *Id.* at 913 (emphasis in
12 original). The loss of “the exclusive use of trade secret information . . . is a real and redressable
13 harm.” *Id.* at 914.

14 **d. Guardant Overwhelming Satisfies This Factor—Likelihood of Success—**
15 **For Issuing A TRO On Its DTSA and CUTSA**

16 The evidence demonstrates that the materials Employee Defendants accessed and stole were
17 trade secrets, and that Defendants’ conduct constitutes misappropriation.

18 Courts in this district and elsewhere have concluded these types of facts demonstrate a trade
19 secrets plaintiff is likely to succeed on the merits of its DTSA and CUTSA claims. *See, e.g., Henry*
20 *Schein, Inc.*, 191 F. Supp. 3d at 1077 (granting TRO and concluding plaintiff was likely to succeed
21 on its DTSA and CUTSA claims because the defendant had “e-mailed and downloaded, to her
22 personal devices, confidential information from [her former employer] before leaving her
23 employment to work at a competitor” and the defendant had signed an agreement with provisions for
24 confidentiality.); *Comet Techs.*, 2018 WL 1990226, at *4 (“Here, Defendant knew or had reason to
25 know that downloading and removing the Da Vinci Project information was theft or, at minimum, a
26 breach of Defendant’s contractual duty to maintain secrecy.”).

1 2. Breach of Contract Claim

2 Guardant also will succeed on its breach of contract claim. To prove breach of contract,
3 Guardant needs to show (1) the existence of a contract, (2) Guardant’s performance, (3) a breach, and
4 (4) damages. *See First Comm'l Mortg. Co. v. Reece*, 89 Cal. App. 4th 731, 745 (2001). Here, there
5 can be no legitimate dispute that the Selewa and Barbacioru CIIAAs are valid contracts, and that
6 Guardant performed by employing both Employee Defendants. Both of Employee Defendants’
7 CIIAAs required they “at all times in perpetuity [] hold all Confidential Information in confidence
8 and [] not disclose, use, copy, publish, summarize, or remove from the premises of the Company any
9 Confidential Information,” with “Confidential Information” broadly defined to include “all
10 information and materials that are confidential, secret, or proprietary (whether or not technical in
11 nature) related to any aspect of the business of the Company.” *See Mancini Decl.*, ¶¶ 6-7, Exs. A, B.
12 The CIIAAs also require the Employee Defendants to return to Guardant and not keep any devices,
13 records, data, or other company documents or property , whether confidential or not, upon termination
14 and to sign a “Termination Certification” to that effect. *Id.* Employee Defendants further agreed that
15 violating the CIIAA “may cause the Company irreparable harm,” that Guardant is “entitled to seek
16 extraordinary relief in court” if they did not comply. *Id.*

17 Here, Guardant’s analysis of its computer systems demonstrated that—contrary to their
18 express promises in their respective CIIAAs—both employees breached their CIIAAs. Barbacioru
19 removed 6,600 files from Guardant’s drives without authorization between January 20 and February
20 7, 2025, while Selewa removed 90 files on January 16, 2025. *Mancini Decl.*, ¶ 9. As discussed above,
21 those files were all Guardant Trade Secrets and Confidential Information. Hence, Employee
22 Defendants breached their CIIAAs.² Also as discussed above, these breaches have caused Guardant
23 significant, irreparable damage.

24 Guardant is likely to succeed on its breach of contract claims as well.

25
26
27
28 ² Barbacioru also refused to return Guardant’s property or sign the Termination Certification,
constituting a separate breach of his CIIAA.

B. Irreparable Harm

Courts “presume that Plaintiff will suffer irreparable harm if its proprietary information is misappropriated.” *Comet Techs.*, 2018 WL 1990226, at *5 (quoting *W. Directories, Inc. v. Golden Guide Directories, Inc.*, 2009 WL 1625945, at *6 (N.D. Cal. 2009)); *see also Apple Inc. v. Rivos, Inc.*, 2023 WL 5183034, at *9 (N.D. Cal. Aug. 11, 2023) (“Generally, harm is presumed when proprietary information is misappropriated.”); *Albert’s Organics, Inc. v. Holzman*, 2020 WL 1332074, at *5 (N.D. Cal. Mar. 23, 2020) (“California courts have presumed irreparable harm when proprietary information is misappropriated.”); *TMX Funding, Inc. v. Impero Techs., Inc.*, 2010 WL 1028254, at *8 (N.D. Cal. Mar. 18, 2010) (same). Given Guardant is likely to prevail on its trade secret misappropriation claims, irreparable harm exists here. *See Lillge v. Verity*, 2007 WL 2900568, at *7 (N.D. Cal. Oct. 2, 2007) (“[T]he risk of losing established customers to defendants’ new business due to defendants’ improper use of plaintiff’s proprietary information would obviously create lasting, irreparable harm.”).

Other factors also indicate Guardant is likely to suffer irreparable harm. “Evidence of threatened loss of prospective customers or goodwill certainly supports a finding of the possibility of irreparable harm.” *Henry Schein*, 191 F. Supp. 3d at 1077 (quoting *Stuhlberg Int’l Sales Co. v. John D. Brush & Co.*, 240 F.3d 832, 841 (9th Cir. 2001)). Here, Employee Defendants took proprietary information relating to several of Guardant’s core screening tests and data sets and then immediately began working at Guardant’s primary competitor; Guardant now faces a substantial risk of losing customers based on Natera’s access to, and use of, Guardant’s proprietary information. *Eldorado Stone*, 2005 WL 5517732, at *4 (“On the issue of irreparable harm, Eldorado will suffer injury in the form of lower sales and potential diminution of market share.”). Moreover, Guardant’s expenditure of years of research-and-development time and millions-of-dollars on testing, data collection, software programming, and analysis further demonstrates Employee Defendants’ misappropriation and disclosure of Guardant’s information will jeopardize Guardant’s competitive position. *See Posdata*, 2007 WL 1848661, at *8 (“The Posdata technology at issue has been developed with substantial company resources and at considerable cost, thus development by InQuadron of this technology or its dissemination may result in irreparable harm to plaintiff.”).

1 **C. Balance of Equities**

2 “The proprietary information at issue belongs to Plaintiff, not Defendant. Thus, Plaintiff has
3 a very strong interest in ensuring that the information is not disclosed. On the other side, Defendant
4 has little interest in disclosing or using the information because such disclosure or use is
5 unauthorized.” *Comet Techs.*, 2018 WL 1990226, at *5 (finding that a TRO “will result in little
6 meaningful hardship to Defendant because the TRO would essentially only require him to abide by
7 existing law regarding the unauthorized use of another’s trade secrets.” (*quoting Pyro Spectaculars*
8 *N., Inc. v. Souza*, 861 F. Supp. 2d 1079, 1092 (E.D. Cal. 2012))).

9 **D. Injunction is the Public Interest**

10 “[T]he public interest is served when defendant is asked to do no more than abide by trade
11 laws and the obligations of contractual agreements signed with her employer. Public interest is also
12 served by enabling the protection of trade secrets.” *Henry Schein, Inc.*, 191 F. Supp. 3d at 1078
13 (*quoting Bank of Am., N.A. v. Lee*, 2008 WL 4351348, at *7 (C.D. Cal. Sept. 22, 2008)); *see also*
14 *Bank of Am.*, 2008 WL 4351348, at *7 (“While California has a strong public policy in favor of
15 competition, this interest yields to California’s interest in protecting a company’s trade secrets.”).
16 That is what Guardant requests here: (1) that the Employee Defendants comply with their contractual
17 and statutory obligations and return the information they stole from Guardant upon departing the
18 company; and (2) that Natera, one of Guardant’s primary competitors, be barred from using or
19 otherwise exploiting Employee Defendants’ theft for its own benefit. The public interest is therefore
20 served by a TRO in this case. *Cf. Morlife, Inc. v. Perry*, 56 Cal. App. 4th 1514, 1520 (1997)
21 (protection of a company’s trade secrets is “fundamental to the preservation of our free market
22 economic system”).

23 **E. Bond**

24 While Federal Rule of Civil Procedure 65(c) states that parties seeking TROs should post a
25 bond, the Rule also “invests the district court with discretion as to the amount of security required, if
26 any.” *Jorgensen v. Cassidy*, 320 F. 3d 906, 919 (9th Cir. 2003) (internal citations omitted). Here,
27 the relief Guardant seeks is only the return of its highly sensitive proprietary information and an order
28 barring Defendants and any of their agents from using that information. *Comet Techs.*, 2018 WL

1 1990226, at *6 (finding no bond necessary as “there is no realistic likelihood of harm to Defendant
2 because Defendant was never entitled to disclose or use the information he took from Plaintiff”).
3 Guardant and the Employee Defendants agreed that in any action for breach of the CIIAA agreements,
4 Guardant “will be entitled to seek extraordinary relief in court, including but not limited to temporary
5 restraining orders, preliminary injunctions and permanent injunctions *without the necessity of posting*
6 *a bond or other security[.]*” See Mancini Decl., Exs. A, B at § 7(f). Accordingly, no bond should be
7 required here. See, e.g., *Henry Schein*, 191 F. Supp. 3d at 1078 (no bond required for a TRO
8 prohibiting defendant from accessing or using plaintiff’s confidential information since it “will not
9 cause any damage to [defendant’s] legitimate business, and further because she agreed, in her
10 employment agreements with [plaintiff], that [plaintiff] may seek injunctive relief without a bond.”);
11 *Comet Techs.*, 2018 WL 1990226 at *6 (same).³

12 **F. Guardant needs expedited discovery to determine the scope of Defendants’ use**
13 **and dissemination of Guardant’s Trade Secrets and Confidential Information**

14 Guardant also requests the Court allow Guardant to conduct narrowly focused, expedited
15 discovery. The standard for expedited discovery is “good cause.” *Semitoool, Inc. v. Tokyo Electron*
16 *Am., Inc.*, 208 F.R.D. 273, 276 (N.D. Cal. 2002). “Good cause may be found where the need for
17 expedited discovery, in consideration of the administration of justice, outweighs the prejudice to the
18 responding party.” *Id.*

19 Here, the discovery Guardant seeks is limited to determining the scope of trade secret and
20 proprietary information Employee Defendants took from Guardant, what they did with those
21 materials, whether they took any other materials Guardant hasn’t discovered, and how those materials
22 have been disseminated, including within Natera. Specifically, Guardant requests be allowed to
23 conduct discovery on:

- 24 • The company property Employee Defendants took from Guardant, including the trade
25 secret and confidential information that is the subject of this action;

26
27 ³ If the Court disagrees, it should require a *de minimus* bond, at most. See, e.g., *Fitspot Ventures,*
28 *LLC v. Bier*, 2015 WL 5145513, at *5 (C.D. Cal. Sept. 1, 2015) (finding a bond of \$5,000 “is
appropriate in light of the fact that it is Plaintiff’s property at issue, and any injury to Defendant is
highly unlikely.”).

- The current location of all Guardant property taken by the Employee Defendants, including the trade secret and confidential information that is the subject of this action;
- Whether, when and what trade secret and confidential information Employee Defendants have disclosed to their new employer, Natera;
- Whether and what trade secret and confidential information Employee Defendants are using in their employment at Natera;
- Whether Employee Defendants received any communications from former Guardant employees that related to Guardant's proprietary information; and
- A forensic computer examination of all computers to which Employee Defendants had access or which the Employees used to access, review, or copy Guardant's proprietary information.

This discovery is appropriate given the Employee Defendants' theft of Guardant's proprietary information and trade secrets, and the serious risk to Guardant from that information being used by one of Guardant's primary competitors, Natera. *See Pyro Spectaculars*, 861 F. Supp. 2d at 1086 (allowing expedited discovery that included forensic computer examinations and depositions before preliminary injunction); *KLA-Tencor v. Murphy*, 717 F. Supp. 2d 895, 898 (N.D. Cal. 2010) (noting court granted plaintiff leave to take expedited discovery along with TRO, including written discovery and oral depositions of defendants); *Grooms v. Legge*, 2009 WL 704644, at *12 (S.D. Cal. Mar. 17, 2009) (same); *see also Comet Techs.*, 2018 WL 1990226, at *6 ("Quickly determining what information Defendant removed from Plaintiff, and whether and how Plaintiff's information is being used by Plaintiff's competitors is essential in order to minimize any harm to Plaintiff's competitive position."). Accordingly, Guardant requests the Court authorize this narrow discovery to determine how far Employee Defendants have disseminated Guardant's Trade Secrets and Confidential Information.

V. CONCLUSION

Employee Defendants obtained and retained some of Guardant's most closely guarded proprietary information and trade secrets. Unless interim injunctive relief is granted, Guardant will suffer immediate and irreparable harm as Guardant's most valuable trade secrets will likely end up in

1 the hands of one of its principal competitors and significantly disadvantage Guardant's ability to
2 compete. Guardant therefore respectfully requests the Court grant this *ex parte* Application for a
3 temporary restraining order, order to show cause why a preliminary injunction should not issue, and
4 order permitted Guardant to conduct expedited discovery.

5 Respectfully submitted,

6 Dated: February 20, 2025

KELLER ANDERLE SCOLNICK LLP

7 By: /s/ Chase A. Scolnick
8 Chase A. Scolnick

9 Attorneys for Plaintiff
10 GUARDANT HEALTH, INC.